EXHIBIT 1

IN THE UNITED STATES DISTRICT
COURT FOR THE WESTERN DISTRICT
OF TEXAS WACO DIVISION

THE TRUSTEES OF PURDUE UNIVERSITY, Plaintiff, v. STMICROELECTRONICS N.V. and STMICROELECTRONICS, INC., Defendants.	Civil Action No. 6:21-cv-00727-ADA JURY TRIAL DEMAND

Expert Report of Greg Jackson

Greg Jackson
July14, 2023

I. INTRODUCTION

1. I have been engaged by counsel for Plaintiff, The Trustees of Purdue University ("Purdue") to provide opinions regarding the creation date of certain electronic files. In particular, I have been asked to opine on the creation date of five Microsoft Word files.

2. This report includes my opinions regarding these files, and if requested, I expect to testify regarding the opinions set forth in this report. I reserve the right to supplement my opinions as a result of further review and analysis, based upon receiving additional information from the parties or the Court, and/or in response to any positions hereafter taken on the issues addressed in this report by Defendants or their expert(s).

3. I am being compensated at the rate of $250 per hour for my time spent on this matter. This compensation is not contingent in any way on the substance of my opinions or testimony in this case, or on the outcome of this case, and has in no way affected my analysis of the issues addressed or the conclusions that I have reached as set forth herein.

II. QUALIFICATIONS

4. I am a licensed Senior Digital Forensics Investigator and e-Discovery professional with over 30 years of experience working within complex management systems for legal, healthcare, insurance, telecom, hospitality and financial organizations. I regularly engage in digital forensic acquisitions, analysis, and e-Discovery in both civil and criminal investigations. Attached to this Declaration as Exhibit A is a true and correct copy of my curriculum vitae.

5. Within the past 10 years, I have analyzed hundreds of terabytes ("TB") of electronic data from computers, servers and mobile devices. This analysis has included the review of structural, system, and application level metadata for Windows operating systems, Apple/Macintosh operating systems, Apple iOS mobile devices and Android mobile devices. I have forensically imaged desktop, laptop and tablet computers, servers, virtual machines, network

attached storage ("NAS") devices, storage area network ("SAN") devices, flash drives and external hard drives including those manufactured by Acer, Apple, Asus, Compaq, EMC, Dell, HP, IBM, Lenovo, Samsung, Seagate, Sony, Toshiba and Western Digital. I have performed electronic recovery of millions of deleted files on both Windows and Mac based computer systems, and analyzed and filtered both active and deleted files relevant to legal actions.

6. With respect to email, I have reviewed, exported and keyword filtered millions of emails from tens of thousands of email accounts stored on Windows and Apple computers, Microsoft Exchange Servers, cloud-based email systems such as AOL, Gmail, Office 365, Yahoo and cloud-based email journaling systems such as the Barracuda Message Archiver and Mimecast.

7. I have also exported, reviewed and key word filtered terabytes of data from Cloud storage systems such as Dropbox, iCloud, Google Drive, Hightail, OneDrive, SharePoint and ShareFile.

8. I have constructed imaging and database systems for managing hundreds of millions of imaged documents, and terabytes of electronic data, and have reviewed, filtered and extracted millions of records from SQL Server, Oracle, and Unix databases.

9. Over the past 10 years, I have collected and analyzed the contents of hundreds of mobile devices, including the analysis of the internal structure of text message databases for both Android and Apple devices, and have extracted and key word filtered over five million text messages from these devices.

III. OPINIONS

10. I was asked to investigate the creation date of five Microsoft Word files sent to me by counsel. Those files are titled chap1.doc, chap2.doc, chap3.doc, chap4.doc, and chap5.doc.[1]

[1] I understand from counsel for Purdue that these files were produced in this litigation at PU0007057-7065, PU0006987-6999, PU00006956-6986, PU0007066-7076, and PU0007178-

Based on a discussion with Dr. James Cooper, I understand that these files were obtained from his MacBook Pro laptop during document collection efforts for this lawsuit and that they represent all or a portion of the PhD thesis proposal of one of Dr. Cooper's students, Dr. Asmita Saha. Dr. Cooper similarly testified about the metadata during his deposition. *See* Cooper Dep. Tr. at 307:1-15.

11. I have investigated the five files provided, and have determined based on the metadata, that all five files were created in 2004. In particular, the files chap1.doc and chap4.doc where created on or about February 29, 2004. The file chap2.doc was created on or about February 26, 2004. The file chap3.doc was created on or about February 7, 2004. The file chap5.doc was created on or about April 10, 2004.

12. Metadata, in essence, is data about data. It's a collection of additional information that gives context to a piece of data, enhancing its usability and management. Metadata can describe the structural aspects of the data, such as file format; administrative details like creation time, access permissions, and copyright; and content-related information, such as a title or keywords.

13. System metadata is like a book's information stored in a library card catalog (or today, a digital catalog). Just as a library card might provide a book's title, its author, the date it was added to the library, and where it is located on the shelves, system metadata provides similar information about a digital file. It identifies the file's name, when it was created or copied onto the current system, when it was last accessed or modified, and where it's stored on an electronic device. This data is managed by the storage device's file system, and updated by the computer's operating system. Certain aspects, such as the creation date, can change if the file is moved or copied to a

---

7183.

different location.

14. Application metadata, on the other hand, is like the information printed on the first few pages of a book, such as the author, the publisher, when it was printed, etc. This data is not about the book's content, but rather, about its production. Similarly, application metadata is data that is embedded within the file by the software that created it. For instance, a Word document may contain metadata about who created it, the date created, date modified, how often it was revised, how much time was spent editing it, etc. This metadata travels with the file, no matter where it is stored or sent, and is thus a reasonably reliable metric to consider when authenticating data, such as when a file was originally created, and when the content of the file was last changed or modified.

IV. CONCLUSION

15. Based on my analysis of the application metadata, I can opine that the files titled chap1.doc through chap5.doc were created within the timeframe of February to April 2004. Although the alphanumeric sequence of the file names do not align directly with the order of creation dates, all dates fall within a narrow timeframe, suggesting a continuous span of work. This chronological consistency further supports the authenticity of the creation dates.

16. My conclusions, as detailed in this report, have been drawn primarily from the application metadata, an element that is generally a reliable source for determining file creation dates in the field of digital forensics. More specifically, with respect to file creation dates, application metadata frequently offers a more accurate and reliable metric than system metadata for identifying a file's original creation date. In contrast to system metadata, application metadata retains its consistency even when a file is transferred or emailed, thereby making it a reasonably reliable source for this analysis.

17. The findings I present herein are based on the data available, and in accordance

with the generally accepted standards within my professional field.

EXHIBIT A

Greg Jackson
1412 Main Street, Suite 612
Dallas, TX 75202
Office: (214) 702-4130
Mobile: (214) 773-4921
greg@jackson.pro

A licensed Senior Digital Forensics Investigator and eDiscovery expert with over 30 years of experience, proficient in navigating intricate management systems for prominent national legal, healthcare, insurance, telecom, hospitality, and financial organizations.

Solid expertise in digital forensic acquisitions, analysis, and eDiscovery across civil and criminal investigations.

PROFESSIONAL HISTORY

- Private Investigator / Digital Forensics Examiner, 2009 to Present
- eDiscovery Consultant, 2005 to present
- Bickel & Brewer, 1987 to 2005
- I&A International, 1994 to 2005
- Ashford Financial Group, 1984 to 1987

SELECT PROJECT EXPERIENCE

- **Data Mining**
  Executed electronic review and analysis of computer systems in numerous cases, including the examination of over 40 terabytes of data for a liquidating bankruptcy estate of a major nationwide mortgage origination company. Provided litigation support for multiple actions against former insiders, Wall Street firms, and associated federal investigations.
- **Computer Forensics**
  Conducted forensic acquisition and analysis on a thousands of desktops, laptops, servers, removable media, and mobile devices; exported petabytes of email from Exchange Server and web-based email systems; filtered and extracted billions of records from SQL Server and Oracle databases.
- **Data Recovery**
  Performed recovery for millions of deleted files on both Windows and Mac-based computer systems, analyzing and filtering files pertinent to legal actions.
- **Metadata Analysis**
  Examined structural and system metadata, document metadata, web page metadata, email message header information, and IP addresses in cases involving discovery misconduct, copyright violations, derogatory blog postings, and identification of web-based file access.

LICENSES AND EDUCATION

Computer Forensics Examiner Course
2009 University of Texas at Arlington

Certified Smartphone Examiner
2018 Paraben Corporation

Licensed Private Investigator
Texas Department of Public Safety - Private Security Board
License number 03443901, Company license number A15843